SUPREMO AMICUS

VOLUME 19 ISSN 2456-9704

CYBERCRIME: A SURVEY FOR PERCEPTION OF ADULTS

By Yatharth Chauhan
From Gautam Buddha University, Greater Noida

Abstract

In today's scenario, cybercrime, criminal activity, has become a matter of great concern across the globe. Primarily, cybercrime is an umbrage committed by the hackers via digital means. Cybercrime could be committed for various reasons say for instance money, political purpose, etc. It has been observed that with the growth as well as development of technology, everything is getting rife with digitization and thus it enhances the chances of ooze of private information. This paper aims at expounding the rationale behind the cybercrime and how Mobile Applications and SIM Swapping contributes to cybercrime. Another intent of this paper is to ascertain the thoughts of common citizens pertaining to cybercrime via questionnaire. The Data which has been collected through questionnaire would be scrutinize both quantitatively as well as qualitatively in great detail.

Keywords: Cyberthreat, Private Information, Digitization, SIM Swapping, Money, Political purpose.

INTRODUCTION

Cybercrime has gained currency under the aura of technology. Since the technology advances, people across the countries have gradually started stowing their personal data digitally in the laptops/computers. Lets say for instance stowing the credentials on google drive or I-cloud. In 2014, according to the International Business Times, almost 4.93 million google accounts were printed on Russian Language Bitcon Security form. Those google accounts were belonged to English, Spanish as well as Russian users. Similarly, whenever customer buys any goods online from any website, numerous option is available to them to make payment for the same say for instance digital wallet, net banking transfer, etc. Thus, he has to supply his personal details. According to the J.P Morgan, trend of payment 2019(Global Insight Report), it has been observed that while making payment for any purpose, 25% of the people preferred digital wallet, 29% of people preferred either debit card or credit card, 17% of the people preferred cash mode, 20% of the people preferred bank transfer and 9% of the people preferred other mode[1]. can we give assurance to ourselves that making payment digitally is devoid of any kind of cyber threat? Can we give assurance to ourselves that stowing data digitally on google drive or I-cloud is devoid of any cyberthreat?

We firmly agree with the fact that advancement of Technology is decorously enriched with numerous benefits including growth as well as development of country but

[1] J.P Morgan, E-commerce Payments Trends in India, India's e-commerce market trends: Huge growth predicted as internet penetration rises, May 10, 2020, 4:48 PM, https://www.jpmorgan.com/merchant-services/insights/reports/india

besides this is an important aspect, require on the part of each and every individual to take into confidence that is to say security of our credentials.

Generally, it has been observed that people usually goes to public cafes for their work. But here on this point an important question tends to arise namely Are people well acquainted with the term keylogger ? As we know that key logger is a kind of malicious act, committed with the intent to get accessibility to the credentials by monitoring or recording all the keys which get struck on keyboard by any person. In other words we could say that keylogger is a kind of software program which is specifically designed with the intent to monitor the keystroke. Keylogger can affect the people adversely. They can easily encrypt the private information via keyboard. Consequently, hackers then get access to the account number, PIN codes, email address as well as their password, accessibility to the password of online gaming accounts, etc. The Notion with respect to keylogger is to get accessibility between two vital aspects that is to say when any key is pressed on the keyboard and another is information which is exhibited on the screen of monitor about the keystroke and this could be attain in various ways say for instance video surveillance, hardware bug in the keyboard, obstruct the input or output, to substitute the driver of keyboard, etc[2].

In United States of America, a similar case has had occurred, there was a businessman named Jeo Lopez, belonged to Florida, had file a suit against the Bank of America, contended that 90,000 Dollars from his bank account had been stolen and when an investigation was conducted for the same it was realized that Mr. Jeo Lopez's computer was enveloped with a malicious program named backdoor coreflood and this malicious program had monitored each and every single key of keyboard, pressed by Mr. Jeo Lopez' and the same had been relocated to the fraudster through internet and hence, it gave rise to the ooze of his username as well as password[3]. This is how he got trapped via keylogger as well as his own negligence. However, it is pertinent to note that the supreme court of Florida rejected the contention of Mr. Jeo Lopez' and said it happened because Mr. Jeo Lopez' did not take any precautions for his credentials.

Cyberbullying is one of the another main, aspect of cybercrime. Cyberbullying, primarily includes sending mean texts or IMs, trying to get access to social media account to lies about someone or with the intent to raise money, creating the nasty webpage of anyone else, etc.

In November, 2019 a case related to cyberbullying was bring into light. A 24-year old boy named Bathula Venkateswarlu, was illegally using the social media profile of a woman and that woman in her complaint contended that he was trying to spill the money from one of her facebook friends by claiming that the money will be used to pay off the medical bills and when the investigation was conducted, it has been detected that Bathula Venkateswarlu has sent link to that woman from one of the phishing, websites and stole her, I'd as well as

[2] Nikoloy Gribennikov, Keyloggers: how they work and how to detect them, Keyloggers Construction, May 14, 2020, 10:17 PM, https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them

[3] "id."

password of the facebook account[4]. Then after impersonating that woman he had started chatting with her friend. That woman also contended that she was unable to get access to her facebook account since September 2019. After all this, is it plausible on the part of us to say that our private information, is out of harm's way? The answer to this question is absolutely No.

RATIONALE AFTER CYBERCRIME

1. To Attain Monetary Purpose

Primarily, cybercriminals resorts to hacking with the intent to gain money. Generally, cybercriminal are rife with major techniques to achieve the said goal that is to say, Infringement of credentials for the purpose of identity theft as well as Attack to inflict fraud on business and under the former, the swindler of the third party contributes to the identity theft and the spill of personal data give platform to the cybercriminals to rupture the credentials of any person so that they could end up with the identity theft whereas under the latter, deflection take place with respect to the fund or money from the targeted account to that account which is controlled by the fraudster and to attain the same they ordinarily deploy various techniques say for instance Phishing, vishing, etc. to spring out the private data[5]. The fraudster will send you an email which exactly looks like that it has come from admissible person but it is not. Such kind of attack is ordinarily invoice. They will either ask you to furnish your credentials with respect to your bank account or alter your bank details. But in reality, those emails primarily comes from cybercriminals with the intent to ruse people in their cyber trap.

2. Political Motive

Another reason is political purpose. Cybercriminals attempts such attack with the purpose to destabilize the normal activity of government, political bodies, etc. The spill of Panama Papers in 2016 is a spellbinding example of it[6]. The Panama Papers implies the slip of 11.5 million confidential documents. And those personal documents belonged to law firm named Mossack Fonseca and the same got published in a German newspaper on 3rd April,2016 Suddeutsche Zeitung. These documents covered the personal financial documents of businessman, politicians, public officials, etc. Almost 2.76 terabytes data were published. Before the slip of data it has been observed that the German newspaper Suddeutsche Zeitung has been contacted by a person John Doe. And even John Doe did not ask for any money but during the conversation names of some public officials, politicians, businessmen had been revealed. This clearly depicts that the spill of Panama Papers is related to Political Motive. Because during the conversation names of some Politicians were also revealed.

Even in 2016 the Russian government tried to demolished the system of democracy during the period of elections in United State of American and when the investigation for the same was conducted it has been realized that

[4] ANI, Telangana Man All Allegedly Hacked Woman's Facebook, Asked friends for Money, Hyderabad, Telangana, May 14, 2020, 11:21 PM, https://www.ndtv.com/telangana-news/telangana-man-allegedly-hacked-womans-facebook-asked-friends-for-money-2127057

[5] Sarah Rutherford, Why do Hackers Commit Cyber Attacks, Fraud Protection and Compliance, May 15, 2020, 9:46 PM, https://www.fico.com/blogs/why-do-hackers-commit-cyber-attacks

[6] Will Kenton, Financial Fraud, The Panama Papers: What you should know, May 17, 2020, 1:10 PM, https://www.investopedia.com/terms/p/panama-papers.asp

Russian government tried to hack the rolls of voters as well as electoral system[7]. The Russian government wanted to debilitate the trust of people in the system of democracy. They wanted to destabilize as well as deranged the government from their legitimate targeted activities. It has to be noted that Russian government not only did it with America. Besides America, there are many other countries namely France, Ukraine, etc. which had been affected by the Russian government.

Are Teenagers into Cybercrime ?

The teens of today's generation are very effectively well versed with the technology. It has been observed from the report of National crime agency in United Kingdom that 61% of hackers were belonged to the age of below 16 and it is pertinent to note that according to the report Australian Bureau of Statistics and crime investigation, it has been observed that cybercrime perpetrated by below the age of 18 have been surged by 26% in the preceding two years and also it has been observed that in Spain almost 3[illegible]0 teens have been dismissed because of their involvement in the cybercrime[8].

To get into this, it is vital that we have to take Traditional Criminology Theory by Gottfredson and Hirschi into meditation[9]. According to this theory, teens who do not have self- control are more likely to commit the cybercrime. In other words, we could say that teens with such kind of characteristics are of impetuous nature. Before attempting they don't ponder the pros as well as cons of that particular aspect that is to, say they act impulsively. Due to lack of requisite brain structure, it become impossible on the part of them to create self-control. Thus, it has been descried that this directly implies getting into the business of cybercrime.

How does sim Swapping contribute to Cybercrime?

Generally, Sim Swapping is a new form of fraud which primarily allows the hackers to purloin your private data of your bank account. Fraudster will block your SIM card and replaced that blocked SIM card with a new SIM card. This technique is also known as SIM splitting. SIM swapper will send you phishing emails. They will try to ruse the person by claiming that they are from health insurer or credit card companies or any other association so that they could get access to your personal data. They also deploy various software to get the same. Then next they will contact to your Mobile service provider and try to deceive the Mobile Service Provider so that they could get a sim card by holding that their sim card is lost or damaged or any other rationale.

Once the SIM Swapper is able to deceived the Mobile Service Provider, they easily get a new SIM card. And once a new SIM card is issued to the fraudster, the SIM card of the targeted victim gets deactivated, now the targeted victim will not be able to receive any kind of information in the cell phone. From this we could easily inferred that the ball is now in the court of SIM Swapper that is to say they have the accessibility now to the

[7] Juan C. Zarate, Democracy, The Cyber Attack on Democracy, May 18, 2020, 10:11 AM, https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html

[8] Teens and Cybercrime, Factors Drive Some Young People to get Involved in Criminal Activities on the Internet, May 23, 2020, 5:30 PM, https://www.buguroo.com/en/blog/teens-and-cyberdelinquency-the-impact-of-low-online-self-control

[9] "id."

personal details including the details of the bank. In such favorable circumstances, the fraudster could easily use the OTP (one Time Password) for any kind of financial transaction.

Recently, in 2019 a case of SIM Swapping was discovered in Mumbai[10]. There was a businessman, who have had received 6 calls on his cell phone between 11.44pm and 1.58am on 27th December as well as 28th December. Among the 6 calls which he had received, 2 calls were from the United Kingdom. Even his SIM card was no more working. Aggrieved by this he called on the service provider and discovered that the SIM card was not working because he himself made a behest to service provider to occlude his SIM card on 27th December around 11.15pm. Then afterwards the service provider gave another new SIM card on 29th December.

In totality there are 28 transactions with respect to the transfer of money into 15 different accounts took place. Even the businessman himself gave the statement that "I was not acknowledged with respect to these transactions because the SIM card was not working. Akbar Pathan, Deputy Police Commissioner, said "Almost 1.86 crore had been relocated from the businessman's current account.

Statistical Facts with respect to Cybercrime in India

Since we know that advancement of technology facilitate necessary growth as well as development. Besides this it is quiet, germane to pay heed to the fact that the more we are into the aura of digitalization, the more we are surrendering our credentials to the innovative cybercriminals. Recently in 2019, a survey was conducted by the Nortion Life Lock Cyber 5afety and the following data has been collected[11].

1. Out of 350 million worldwide cybercrime victims, India's victims of cybercrime stands out to be 131.2 million.
2. Due to cybercrime India has lost almost 1.24 trillion amount.
3. Out of 131.2 million victims of cybercrime, 63% of Indians are exposed to cybercrime financially.
4. 63% Indians do not know what they should do if circumstances like where their identities are stolen, appears to them.
5. 73% Indians are well versed with the fact that their identities will going to be stolen by the cybercriminals.

In 2019, an official annual report with respect to cybercrime by cyber securities venture was published[12]. It clearly states that cybercrime will cost the world 6$ trillion by 2021. It is predominant to note that this will facilitate a shift on large scale with respect to the economic wealth and thus affecting the field of Investment as well as Innovation. Steve Morgan, founder as well as Editor-in-chief at cyber security venture, contended that

[10] Saurabh Gupta, How 6 Missed calls left Businessman Robbed of nearly 2 crore, Mumbai, May 24, 2020, 3:19 PM, https://www.ndtv.com/mumbai-news/how-6-missed-calls-left-mumbai-businessman-robbed-off-rs-1-86-crore-1972131

[11] Riju Mehta, Nortion Life Lock Cyber safety Insight Report, Cybercriminals Stole Rupees 1.2 Trillion from Indian in 2019: Survey, May 25, 2020, 8:41 PM, https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019-survey/articleshow/75093578.cms

[12] Herjavec Group, Cybersecurity venture Official Annual Cybercrime Report, Cybercrime Damages $6 Trillion by 2021, May 29, 2020, 10:31 Pm, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

cybercrime covers the numerous vital aspects namely credentials, personal financial data, Intellectual property which is being stolen, Production cost, Damaged cost, Money, etc[13].

How does Mobile Applications contribute to cybercrimes?

Another important aspect which blossoms the cybercrime is that various mobile apps have become the source for cybercriminals with the intent to achieve the private data including details of bank. And such apps include Malware, Coat-trailing trojans, etc. contribute to cybercrime. Such kind of software could be easily pierce into the cell phone and could encrypts the data. There are primarily three ways deploy by the cybercriminals to extract the private data from mobile or laptops that is to say through browser or applications or internet network which claims to provide free WIFI. The Aarogya Setu Application, designed in the name of covid-19, could be cite as an example[14]. The cybercriminals are sending the phishing messages or phishing emails in the name of Aarogya Setu Application so that they could be able to steal the private Data. Fraudster are sending illegitimate emails or messages say for instance 'check who all are infected by covid-19', 'How to use Aarogya Setu Applications' etc. It was also observed that cybercriminals are dispatching the phishing emails which are appearing to the people that they are originating from World Health Organization.

Not only this, cybercriminals are trying to ruse the people by providing free Netflix passes in the name of covid-19[15]. Even some of the people are getting the link on the WhatsApp that to get entitled to free subscription of Netflix, click on this link. But in reality, it is nothing but only a scam to trick people so that cybercriminals could get the credentials of people. It has been observed that one of the spoke person of the Netflix has given a confirmation that we have not accord any free subscription of Netflix. This clearly shows that free subscription is a kind of scam for common citizen to deceive them.

Methodology

The concept of cybercrime have had been elaborated in great detail. Along with this the rationale after the cybercrime have had also been discussed. And the another important aspect that is to say to find out the opinion of the common citizens pertaining to cybercrime, the data for the same has been collected in the form of questionnaire. And the same had been scrutinized both quantitatively as well as qualitatively. Some general questions related to cybercrime were asked in the questionnaire. All the respondents were assured of the confidentiality.

Discussion and Inferences

Demographic Profile

In this survey the data has been collected from the undergraduate students, Postgraduate students and those who does

[13] "id."

[14] [14] PTI, Technology, Phishing attacks in the name of Aarogya Setu App increasing :CERT-in, May 28, 2020, 11:11 PM, https://www.thehindu.com/sci-tech/technology/phishing-attacks-in-name-of-aarogya-setu-app-increasing-cyber-agency/article31601964.ece

[15] HT Correspondent, Beware of Free Netflix passes messages it's a scam, May 28, 2020, 12:34 AM, https://tech.hindustantimes.com/tech/news/beware-of-free-netflix-passes-messages-it-s-a-scam-story-ABArM51Lv4V0l9IwB2jJaJ.html

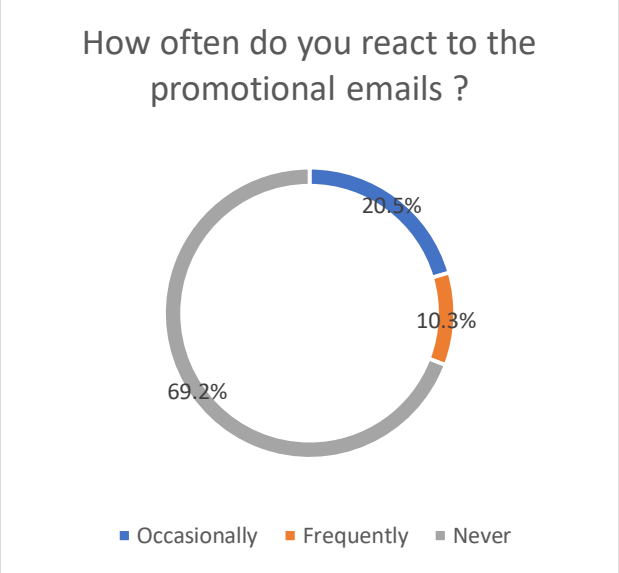
job. There is almost an equal distribution of both male as well as female. Various other aspects of the questionnaire are now discussed individually one by one.

Do you think that making payment via Digital wallet is devoid of any cyber threat?

To this question, it was observed that 82.1% of the respondents said making payment via digital wallet is not free of any cyber threat whereas 17.9% of the respondents said it is. This clearly depicts that 82.1% of people are well versed with the fact that digital wallet holds cyber threat. It means they are cautious whenever it comes to hit digital wallet for payment and can scrutinize the situation. But when it comes to latter category that is say 17.9% of the respondents, it gives rise to exigency that people should be heedful to cybercrime. The fact that as of now they are not vulnerable to cybercrime could not be taken as a justification for latter one. The chief ratiocination is that we cannot predict about the numerous aspects of cybercrime. Hence, we need to be careful.

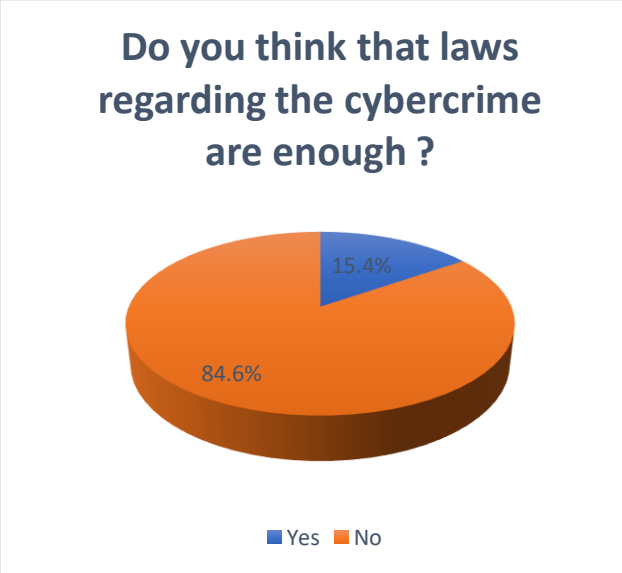
How often do you react to the promotional emails?

This is the another question which was asked in the questionnaire and it was asked in the three category that is to say occasional category, frequently category and never category. It was found that 20.5% of the respondents went for occasional category, 69.2 % of the respondents went for never and 10.35 went for frequently category. This shows that 69.2% of the respondents are well aware that promotional emails is threat in the form of cybercrime. Because promotional emails is a kind of weapon deploy by the cybercriminals in the form of phishing so that they could get access to personal data. But when it comes to occasionally as well as frequently category, people should become cautious with respect to challenges of cybercrime. They should avoid such kind of illegitimate emails and if the circumstances are such that it is quite crucial to react on such emails then before hitting the response they should scrutinize the integrity of such emails.



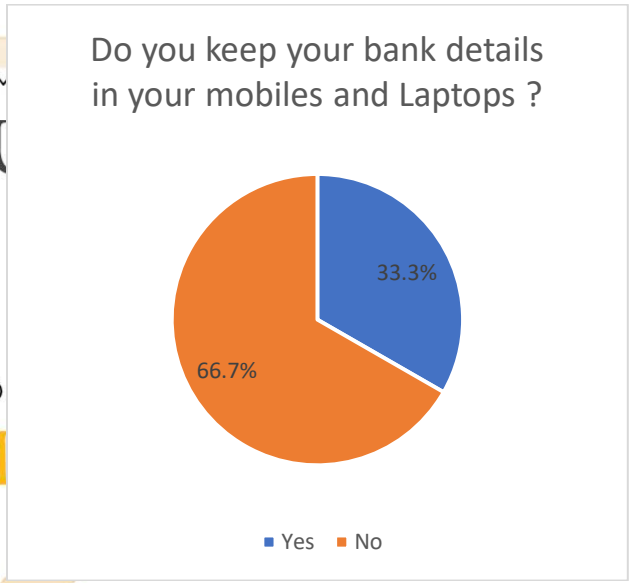
Can we say that laws regarding the cybercrime are enough?

This is the another question which was asked in the questionnaire and it was observed that 84.6% of the respondents said we need more stringent laws to curb the cybercrime at the earliest whereas 15.4% of the respondents said the laws regarding the cybercrime are suffice. This shows that the former category is more conscious with respect to cybersecurity. An important noteworthy aspect is that we cannot let the cybercrime to prevail over the advancement of technology. Thus, we need to tefurbish the cyberthreat at the earliest. The latter one needs to understand the relation of stringent laws with respect to cybercrime. Because we required an indestructible cybersecurity.



Do you keep your bank details in your mobiles and laptops?

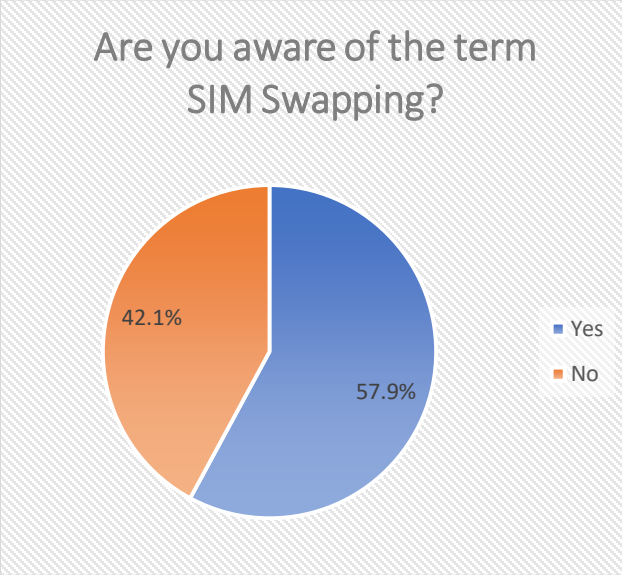
It was found that 66.7% of the respondents went against the motion whereas 33.3% of the respondents went for the motion. From this data, we could inferred that the former category is across to the fact that if we surrender our personal financial information in the cell phones or laptops then the same could be easily compromised by any kind of software say for instance malware with the intent to gain unauthorized access to laptops or computers. The latter category firmly holds that private data in mobiles or laptops are devoid of any cyberthreat. They have to understand that data could be easily fetched by the cybercriminals via any kind of techniques. So, it is cardinal that they should become prudent against cybercrime. Because ignorance on the part of us can lead to uproot of our credentials.



Are you aware of the term SIM swapping?

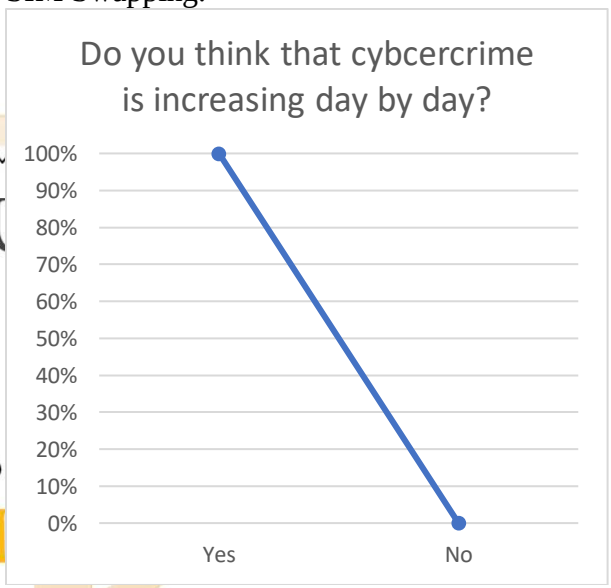
This is the another question which was asked and it was found that 57.9% of the respondents are well aware about the SIM Swapping whereas 42.1% of the respondents are not aware about the term SIM Swapping. Thus, it is important on the part of latter one to become familiar with the term SIM Swapping. Hence, there is an exigency to create awareness with respect to numerous aspects of cybercrime among the common

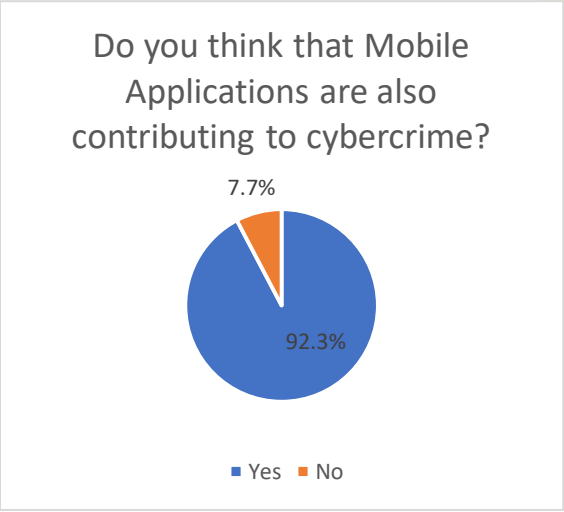
citizens. The more we create the awareness, the more we are able to control or restrict the cyberthreat.



Do you think that cybercrime is increasing day-by-day?

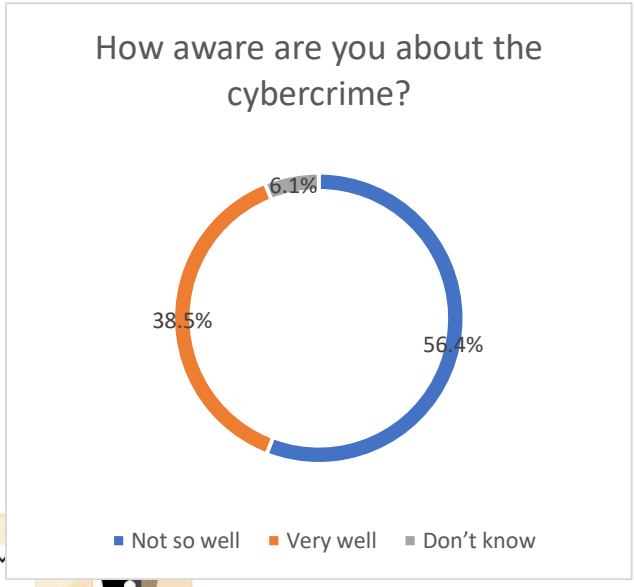
And to this, we have had received 10[illegible]% vote in favor of the question. It means that people are cognizant that cybercrime is scaling up. It is to be noted that though people are conscious about the fact that cybercrime is scaling up. Although people are conscious about the fact that cybercrime is increasing day-by-day besides this it is pertinent to note that cybercrime holds various parts. Being aware about the fact that cybercrime is increasing day-by-day will not suffice. Therefore, it is important that they should aware about the sub-parts of the cybercrime. As in the above question which talks about the SIM Swapping, we could see that 42.1% of the respondents are not aware about the SIM Swapping.





Do you think that Mobile Applications are contributing to cybercrime?

To this question it was observed that 92.3% of the respondents went for the motion whereas 7.7% of the respondents went against the motion. As we could take the example of Aarogya Setu App, Cybercriminals are sending illegitimate emails (phishing) in the name of Aarogya Setu App to ruse the people. Hence, before deploying any such applications people should analyze the same in detail.



How aware are you about cybercrime?

This question has been asked in three category that is to say very well, Don't know and Not so well. And it was observed that 56.4% of the respondents went for very well, 38.5% of the respondents went for very well and 6.1% of the respondents went for Don't know. Thus, from this we could inferred that awareness regarding the cyberthreat is must. Because if we are aware about the challenges of cyberspace then we could be able to take the requisite precautions against the cybercrime. Unless we are not across to the cybercrime in detail then Law in such situation is equivalent to vain. Mainly, cybercrime takes place because of not being cautious. As in the aforesaid case of Mr. Lopez with respect to key logger, the supreme court of Florida said Mr. Lopez had has suffered loss because of his own negligence.

How do you feel about your information when you are online?

This question is primarily asked in four category that is to say Safe, very safe, not safe and don't know. And it was found that 40% of the respondents contended that they don't feel safe with respect to their private information when they are online, 55% of the respondents said that they feel safe about their information when they are online, 5.1% of the respondents don't know that whether their information is protected or not and none of the respondents went for very safe. This implies that 55% of the respondents do not feel any kind of inconvenience with respect to information. But still they need to safeguard their credentials because the negligence on the part of us could create a room for cybercriminals. But 40% of the respondents knows that storing the data digitally can lead to leakage of the same or in other words we could say that they are not in a favor of uploading the data whereas when it comes to 5.1% of the respondents we could see the uncertainty because they don't know whether uploading the data is reasonable or

not. An important noteworthy point is that respondents are well aware that it is not very Safe to upload the private information. Hence, we need to be careful.

Conclusion

As we know that everything has its own pros as well as cons. Similarly, when it comes to technology, we could say that technology facilitate the progress of a country. But on the other hand, we cannot disregard the cons of the same. In other words, it means we cannot let the cons of technology to prevail over the pros of technology. Because we know that the area of technology is vulnerable to cyberthreat. Thus, on the basis of the data which has been collected via questionnaire, we could say that mainly cybercrimes take place because of the negligence on the part of we people. We need to focus on two aspects that is to say at first, we have to create awareness with respect to cybercrime among the people, we have to educate them about the types of cybercrime and how we can prevent ourselves from becoming immune to cyberthreat. Secondly, before reacting to any kind of emails, it is necessary that its integrity should be taken into confidence. Because the more we will become aware about the cybercrime, the less we will be prone to cybercrime.

*****